CyberRes

Article

ArcSight's Latest and Greatest

New Features of ArcSight 2022.1

ArcSight 2022.1: Threat Research and Smart Storage

General Availability—ArcSight 2022.1 release

We are excited to announce the general availability of ArcSight 2022.1! With our latest release, ArcSight offers columnal/shared storage to provide smart and cost-effective log storage to organizations. Customers can tie storage costs directly to business needs by provisioning the right amount of computer resources for queries and the right amount of storage resources for data. Separating computing resources from data storage brings flexibility, elastic scalability, operational simplicity, and intelligence to the log management needs of modern SOCs.

ArcSight's smart database keeps the primary copy of your data in the communal storage, while the local cache serves as the secondary copy. Adding and removing nodes does not redistribute the primary copy. This shared storage model enables elasticity, making it both efficient and cost-effective to adapt the cluster resources to fit the usage pattern of the cluster. If a node goes down, other nodes are not impacted. Node restarts are super-fast and no recovery is needed.

There is no need to keep track of and load/unload long term-retention event data explicitly. The ArcSight database can bring them automatically to the cache on demand and move them out at rest.

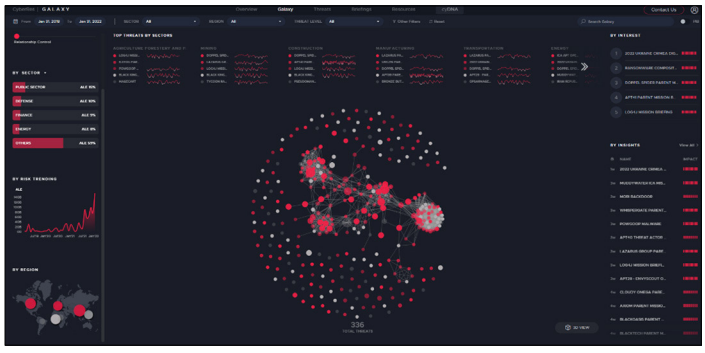

Figure 1. CyberRes Galaxy

Introducing Galaxy Threat Acceleration Program—Basic (GTAP Basic). To complement the functionality of our new threat research program CyberRes Galaxy (released earlier this year), CyberRes has provided ArcSight customers with added interoperability between ArcSight SIEM and Galaxy's curated threat intelligence. ArcSight ESM customers are entitled to install GTAP Basic, which automatically incorporates threat monitoring content for ArcSight. GTAP Basic offers increased coverage against modern threats and campaigns and grants better visibility of industry threats.

CyberRes Galaxy Threat Acceleration Plus (GTAP+) is the premium version of our threat intelligence feed, specifically built for ArcSight Enterprise Security Manager. It incorporates insights from Galaxy's threat research network and provides ArcSight customers with proactive defenses. It increases your coverage against modern threats and threat campaigns by providing more visibility, reducing false positives, and automating threat response.

Galaxy's superior content facilitates out-of-the-box threat detection and response for ArcSight ESM and powers advanced implementation of ATT&CK and D3FEND countermeasures. It provides threat monitoring content that's always on and always up to date. It eliminates blind spots and helps stop breaches before they occur, packaged in a solution that can be installed and operational within minutes.

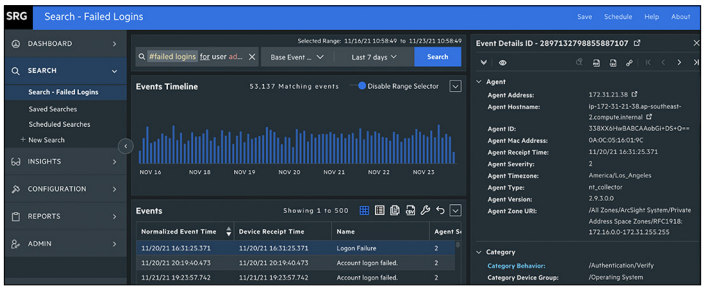

Figure 2. ArcSight SIEM as a Service event detail panel

Fearlessly shift to the cloud with ArcSight SIEM as a Service—We have introduced log management and compliance capabilities as a service to provide a no-hassle security experience by eliminating the cost of buying, installing, and managing servers and simplifying and empowering security operations. There is minimal up-front cost when switching to SaaS and little to no maintenance cost. The ArcSight team takes care of all the servers, hardware, and maintenance on behalf of the customer to eliminate security infrastructure concerns. With auto-updates, customers can run on the latest and greatest versions and benefit from the capability improvements immediately.

As part of our mission to elevate security operations, ArcSight SaaS offers an intelligent, holistic security operation stack with advanced threat hunting, log management, and compliance capabilities in a scalable, no-hassle environment. It provides a very detailed view into exactly what is happening in an organization by turning data into visualizations and actions.

With the latest ArcSight SOAR 3.2 release, we have added 20 more plugin integrations, including threat intelligence databases, cloud services, and IT service managers. We have also developed 16 new playbooks to help customers orchestrate and automate their incident response and speed up case management needs. New dashboards and reports have been added, covering open cases, closed cases, integration history, and integration summary. In addition, SOAR reports now have the same look and feel as the rest of the ArcSight portfolio.

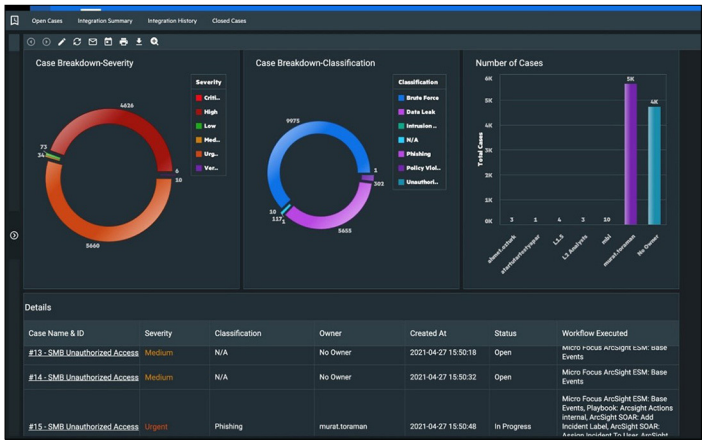

Figure 3. ArcSight SOAR reports and dashboards

We are also happy to report that our commitment to bringing simplicity and efficiency to security operations is being recognized by both market analysts and our customers. ArcSight was recently named an innovative leader that's outperforming the SIEM market in the GigaOm Radar for SIEM. We were also named a Leader in the KuppingerCole Leadership Compass for Intelligent SIEM Platforms. Furthermore, Micro Focus was recently recognized as a 2021 "Customers' Choice" in the Gartner Peer Insights™ 'Voice of the Customer' for SIEM for the ArcSight product solution.

ArcSight 2022.1 features new releases of:

- ArcSight SIEM as a Service
- ArcSight ESM 7.6
- ArcSight Intelligence 6.4
- ArcSight Fusion 1.5
- ArcSight Recon 1.4
- ArcSight SOAR 3.2
- Transformation Hub 3.6
- ArcSight Management Center 3.1
- ArcSight SmartConnectors 8.3

The key features and improvements of our ArcSight 2022.1 release are listed below. Please refer to the individual release notes (cited in this document) for more complete information.

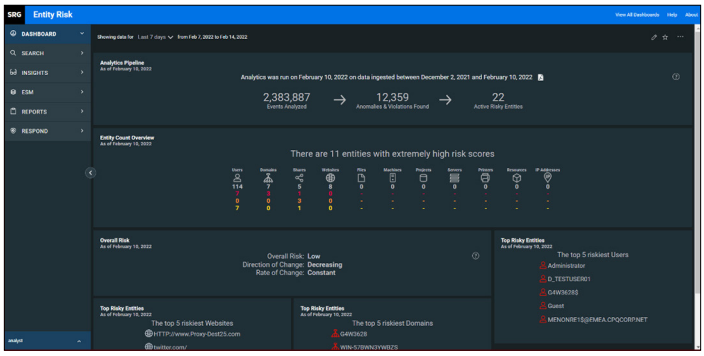

Figure 4. Additional ArcSight Intelligence widgets added to Fusion Dashboard

ArcSight Platform

Key Highlights

- **ArcSight smart log storage** brings intelligence, scalability, flexibility, elasticity, and time & cost effectiveness to storage needs.
- **ArcSight SIEM as a Service Log Management and Compliance** capabilities to fearlessly shift to Micro Focus hosted cloud services.
- **Cloud-native deployment in Azure and AWS** to bring flexible deployment options and decrease hardware requirements for the overall ArcSight portfolio.
- **Simplified reporting for MSSP customers** to automatically perform quarterly reporting.
- **Galaxy Threat Intelligence Feed** to provide curated threat intelligence aligned with our free online Galaxy program, to enable quick detection of threats.
- **ArcSight Fusion 1.5**, which includes a new capability for MSS Partners that enables them to easily analyze and issue reports on their daily and monthly EPS usage.
- **20 new SOAR integrations**, including threat intelligence databases, cloud services, and IT service managers.
- **Pixel perfect ArcSight SOAR reports** to visualize desired reports and turn data into visualizations.
- **16 new SOAR playbooks** to empower SOCs with automated orchestration.
- **Log4j upgrades**, including previously-released patch fixes to address Log4j vulnerabilities.

ArcSight ESM 7.6

Key Highlights

- **Integration with Active Directory (AD)** enables SOCs to manage their ArcSight ESM user/group memberships through their AD users and groups.
- **Enhanced SSO** in Fusion, to better support external authentication sources (e.g., Microsoft 365).
- **Notification management** now enables you to clear notifications at an individual or group level.
- **Improved list performance** in Distributed Mode installations.
- **New APIs** for rules and lists.
- **Currency updates** to Java, SQL, Kafka, and OS.
- **Stability, security, and performance** enhancements.

ArcSight Recon 1.4

Key Highlights

- **ArcSight smart log storage** brings intelligence, scalability, flexibility, elasticity, and time & cost effectiveness to meet storage needs.
- **Scheduled searches** to save time spent searching, analyzing, and threat hunting.
- **Search Query and Search Criteria** to save the query and re-use it again and again as needed.
- **Event Integrity check** to identify modifications and corruptions on the data.
- **License enhancements** to support MSSPs with reporting needs.
- **PCI, ITGOV compliance packages** to ease the burden of compliance reporting.
- **Logger to Recon Migration tool** to migrate Logger customers to Recon 1.4.
- **Backup & Restore of Event data** to be available when needed.
- **90-day Recon Free Trial** is available to customers.

Enhancements

- Scheduled Searches
- Data Quality Dashboard improvements
- Daylight Saving Time enhancement
- AWS and Azure deployment enhancements

ArcSight SIEM as a Service Log Management and Compliance

Key Highlights

- **User-friendly search** displays grid or message views and a time-based histogram.
- **Search time horizon expression dynamically** to derive search time horizon from user-defined expression.
- **Syntax highlighting** for improved search command readability.
- **Raw message view** for analysts to inspect original, unformatted event logs.
- **Event detail panel** for detailed inspection of selected events.
- **Unified platform** to enable routing, filtering, and storage for all ArcSight products.
- **Outlier detection** to visualize deviations from baseline host behavior metrics.

- **Data Quality Dashboard** to display detailed information about the gap between Device Receipt Time from the raw event, versus the time when the event persisted.
- **New user preferences** for search parameters, display formats, and limits.
- **Independent retention periods per storage group for up to 10 groups**, allowing sets of logs to be retained for different periods and improving search performance.
- **Pixel perfect reports and interactive dashboards** to create, edit, publish, and visualize desired reports in order to increase visibility across the security landscape.
- **100+ out-of-the box reports/dashboards**, covering cloud, monitoring, and OWASP.
- **Import and export of reports, dashboards, and related content** to simplify sharing and reviewing.
- **Data modeler** to provide an integrated view and understanding of all the data available in a customer's environment.

ArcSight SOAR 3.2

Key Highlights

- **20 new SOAR integrations**, including threat intelligence databases, cloud services, and IT service managers.
- **Pixel perfect reports for SOAR** to visualize desired reports and turn data into visualizations.
- **16 new SOAR playbooks** to empower SOCs with automated orchestration and help speed up incident response.
- **Cloud-native deployment in Azure and AWS** to provide flexible deployment options and decrease hardware requirements.

ArcSight Intelligence 6.4

Key Highlights

- **MITRE ATT&CK coverage documentation** enables improved understanding of the value of data sources to detect types of threats.
- **New Fusion dashboard widgets** improve the visual threat hunting experience.
- **Adoption of Fusion masthead** creates a more cohesive UI.

ArcSight Transformation Hub 3.6

Key Highlights

- **Performance improvements** and minor **bug fixes**.
- **Detailed documentation** available here.

ArcSight Management Center 3.1

Key Highlights

- **Performance improvements** and minor **bug fixes**.
- **Detailed documentation** available here.

ArcSight SmartConnectors 8.3

Key Highlights

- **New Galaxy Threat Acceleration Program Plus (GTAP+) SmartConnector** connects to Galaxy's premium curated threat intelligence feed to facilitate automated defense.
- **New Galaxy Threat Acceleration Program Basic (GTAP Basic) SmartConnector** connects to Galaxy's basic threat intelligence feed, available to ArcSight customers at no additional charge.
- **Documentation** for reference of ArcSight Connectors.

ArcSight Logger 7.2 (ArcSight 2021.1 Release)

Key Highlights

- **MySQL upgrade** to 5.7.21 for enhanced security.
- **Enhanced Search UI** improves peer search, saved results, and response time.
- **Recon search** of Logger event data is now enabled.
- **One-step upgrade** from any supported version (v6.6 and above) to v7.2.

ArcSight Logger 7.2.1 (Released December 2021)

- Maintenance release addressing security vulnerabilities and other issues found in Logger 7.2.

ArcSight Documentation

Release Notes

- ArcSight Platform 22.1
- ArcSight SaaS
- ArcSight ESM 7.6
- ArcSight Intelligence 6.4
- ArcSight Recon 1.4
- ArcSight SOAR 3.2
- Transformation Hub 3.6
- ArcSight Management Center 3.1
- ArcSight SmartConnectors 8.3
- ArcSight Logger 7.2

Is Your ArcSight Version up to Date?

Product Name	Newest Version
ArcSight Platform	22.1
ArcSight ESM	7.6
ArcSight Intelligence	6.4
ArcSight Recon	1.4
ArcSight SOAR	3.2
ArcSight Logger	7.2
Transformation Hub	3.6
ArcSight Management Center	3.1
ArcSight SmartConnectors	8.3

Learn more at
www.arcsight.com

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes

A Micro Focus line of business